Claims

[c1] What is claimed is:

1. An authentication method used in a digital versatile disk (DVD) system for generating an authentication code according to an inquiring code so as to authenticate a playback device, the inquiring code comprising a first portion and a second portion both with at least one bit;

the method comprising:

generating a first sub-authentication code according to the first portion of the inquiring code;

generating a second sub-authentication code according to the second portion of the inquiring code; and

combining the first sub-authentication code and the second subauthentication code to form the authentication code.

[c2] 2. The authentication method of claim 1, wherein each of the inquiring code and the authentication code has bit length of eight, and each of the first portion of the inquiring code, the second portion of the inquiring code, the first sub-authentication code, and the second sub-authentication code has bit length of four.

[c3] 3. The authentication method of claim 2, wherein a mapping relationship between the first sub-authentication code, the second sub-authentication code, and the authentication code conforms to a pre-table defined in a specification of the digital versatile disk system.

[c4] 4. The authentication method of claim 2, wherein a mapping relationship between the first sub-authentication code, the second sub-authentication code, and the authentication code conforms to a post-table defined in a specification of the digital versatile disk system.

[c5] 5. An authentication circuit used in an authentication process of a digital versatile disk (DVD) system for generating an authentication code according to an inquiring code so as to authenticate a playback device, the inquiring code comprising a first portion and a second portion both with at least one bit;

the authentication circuit comprising:

a first encoder for generating a first sub-authentication code according to only the first portion of the inquiring code; and

a second encoder for generating a second sub-authentication code according to only the second portion of the inquiring code;

wherein the authentication code is generated according to the first sub-authentication code and the second subauthentication code.

[c6] 6. The authentication circuit of claim 5, wherein each of the inquiring code and the authentication code has bit length of eight, and each of the first portion of the inquiring code, the second portion of the inquiring code, the first sub-authentication code, and the second sub-authentication code has bit length of four.

[c7] 7. The authentication circuit of claim 6, wherein a mapping relationship between the first sub-authentication code, the second sub-authentication code, and the authentication code conforms to a pre-table defined in a specification of the digital versatile disk system.

[c8] 8. The authentication circuit of claim 6, wherein a mapping relationship between the first sub-authentication code, the second sub-authentication code, and the authentication code conforms to a post-table defined in a specification of the digital versatile disk system.